




# **DEVICE AND METHOD FOR PROCESSING IMAGE**

**Patent number:** JP2001203878  
**Publication date:** 2001-07-27  
**Inventor:** KAMIJO KOICHI; MORIMOTO NORISHIGE;  
 TONEGAWA SATOKO  
**Applicant:** IBM  
**Classification:**  
 - international: **H04N5/91; G06T1/00; G06T9/00; H04N1/387;  
 H04N1/40; H04N1/41; H04N7/30; H04N5/91; G06T1/00;  
 G06T9/00; H04N1/387; H04N1/40; H04N1/41;  
 H04N7/30; (IPC1-7): H04N1/387; G06T1/00; H04N1/40;  
 H04N1/41; H04N5/91; H04N7/30**  
 - european: G06T1/00W6C; G06T9/00T  
**Application number:** JP20000012520 20000121  
**Priority number(s):** JP20000012520 20000121

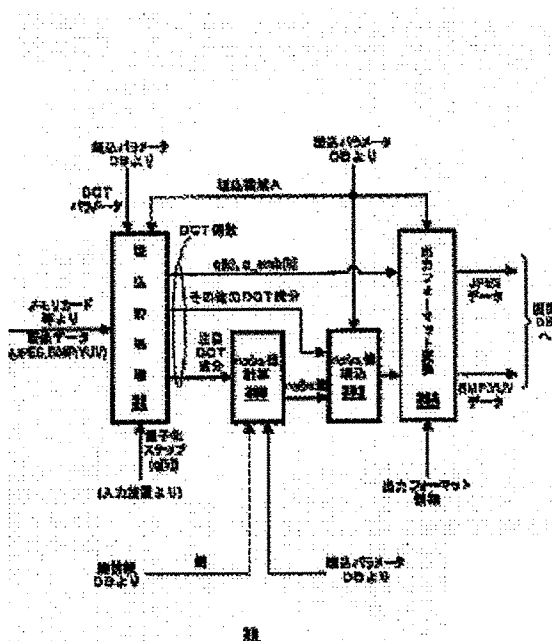
Also published as:

 US7046817 (B2)  
 US2001010729 (A1)  
 GB2359211 (A)

Report a data error here

## **Abstract of JP2001203878**

**PROBLEM TO BE SOLVED:** To prevent embedded authentication information from being lost, even if quantizing processing is performed after the authentication information is embedded.  
**SOLUTION:** A pre-embedding part 32 converts the value of image data, so that the value after quantizing processing can not be changed by an error added by embedding processing of embedded data. A hash value calculating part 300 calculates a hash value from image data and key information and a hash value embedding part 302 embeds the hash value in the image data. An output format converting part 304 generates JPEG data, by applying quantizing processing or the like to the image data embedded with the hash value.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2001-203878  
(P2001-203878A)

(43)公開日 平成13年7月27日(2001.7.27)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)	
H 0 4 N	1/387	H 0 4 N	1/387	5 B 0 5 7
G 0 6 T	1/00		1/41	B 5 C 0 5 3
H 0 4 N	1/40	G 0 6 F	15/66	B 5 C 0 5 9
	1/41	H 0 4 N	1/40	Z 5 C 0 7 6
	5/91		5/91	P 5 C 0 7 7
審査請求 有 請求項の数15 O L (全 25 頁) 最終頁に続く				

(21)出願番号 特願2000-12520(P2000-12520)

(22)出願日 平成12年1月21日(2000.1.21)

(71)出願人 390009531

インターナショナル・ビジネス・マシー  
ズ・コーポレーションINTERNATIONAL BUSIN  
ESS MASCHINES CORPO  
RATIONアメリカ合衆国10504、ニューヨーク州  
アーモンク (番地なし)

(74)代理人 100086243

弁理士 坂口 博 (外1名)

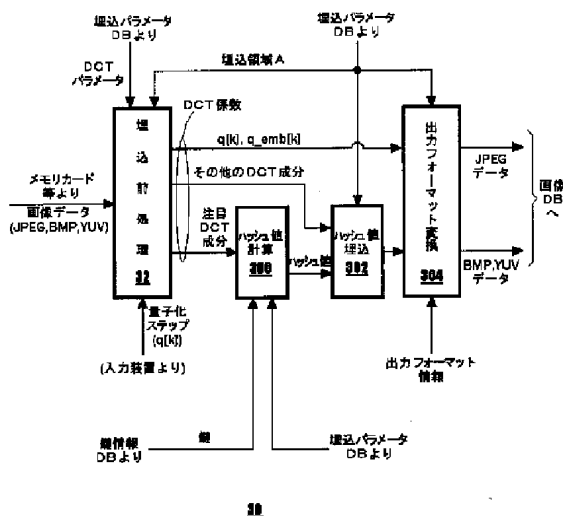
最終頁に続く

(54)【発明の名称】 画像処理装置およびその方法

(57)【要約】

【課題】 認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがないようにする。

【解決手段】 埋込前処理部32は、埋め込みデータの埋め込み処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する。ハッシュ値計算部300は、画像データと鍵情報からハッシュ値を計算し、ハッシュ値埋込部302は、画像データにハッシュ値を埋め込む。出力フォーマット変換部304は、ハッシュ値が埋め込まれた画像データを量子化処理などし、J P E Gデータを生成する。



【特許請求の範囲】

【請求項1】所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換手段（302）と、  
画像データに対して前記所定の処理を行う処理手段（300、302）と、  
前記所定の処理がなされた画像データを量子化処理する量子化手段（304）とを有する画像処理装置。

【請求項2】前記処理手段は、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い（50）、  
前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出手段（60）をさらに有する請求項1に記載の画像処理装置。

【請求項3】前記変換手段は、  
画像データに含まれる画素それぞれの形式を変換する形式変換手段（326、330）と、  
前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節手段（332）とを有し、  
前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す請求項1に記載の画像処理装置。

【請求項4】前記処理手段は、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う請求項1に記載の画像処理装置。

【請求項5】前記処理手段は、所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算手段（300）と、  
計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理手段（302）とを有する請求項4に記載の画像処理装置。

【請求項6】前記画像データに埋め込まれた埋込データを検出する検出手段（30）をさらに有する請求項4または5に記載の画像処理装置。

【請求項7】前記量子化された画像データを逆量子化する逆量子化手段（422）と、  
前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出手段（400）と、  
前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算手段（402）と、  
前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出手段（404）とを有する請求項5に記載の画像処理装置。

【請求項8】所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換し、

画像データに対して前記所定の処理を行い、  
前記所定の処理がなされた画像データを量子化処理する画像処理方法。

【請求項9】所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換ステップと、  
画像データに対して前記所定の処理を行う処理ステップと、  
前記所定の処理がなされた画像データを量子化処理する量子化ステップとをコンピュータに実行させるプログラムを記録した記録媒体。

【請求項10】前記処理ステップは、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い、  
前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出ステップをさらに有する請求項9に記載の記録媒体。

【請求項11】前記変換ステップは、  
画像データに含まれる画素それぞれの形式を変換する形式変換ステップと、  
前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節ステップとを有し、  
前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す請求項9に記載の記録媒体。

【請求項12】前記処理ステップは、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う請求項9に記載の記録媒体。

【請求項13】前記処理ステップは、  
所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算ステップと、  
計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理ステップとを有する請求項12に記載の記録媒体。

【請求項14】前記画像データに埋め込まれた埋込データを検出する検出ステップをさらに有する請求項12または13に記載の記録媒体。

【請求項15】前記量子化された画像データを逆量子化する逆量子化ステップと、  
前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出ステップと、  
前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算ステップと、  
前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出ステップとを有する請求項13に記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、著作権情報などの認証情報（埋め込みデータ）を埋め込んだ画像データ等を、圧縮のために量子化しても、埋め込まれた認証データが失われないようにした画像処理装置およびその方法に関する。

【0002】

【従来の技術】例えば、国際公開WO97/49235号公報（文献1）は、ピクセル・ブロック・コーディング（Pixel Block Coding；PBC）により、画像データ等のコンテンツデータに著作権情報など（以下、一般的に認証情報あるいは埋め込みデータ等とも記す）を、視覚的に感知できないように埋め込む方式（以下、このようにコンテンツデータに感知できないように認証方法を埋め込む方式を「エレクトロニックウォーターマーキング方式」とも記す）を開示する。

【0003】また、国際公開WO98/116928号公報（文献2）は、文献1等を開示されたエレクトロニックウォーターマーキング方式を応用して、画像データの改変を禁止し、著作物を有効に保護する方法を開示する。また、特開平10-164549号公報（文献3）は、文献1等を開示されたエレクトロニックウォーターマーキング方式を改良し、画像データに認証情報を一体不可分に埋め込むことにより、画像データの改変を検出する方法を開示する。

【0004】また、これらの文献の他、特開平09-151747号公報、特開平10-83310号公報、特開平10-106149号公報、特開平10-161933号公報、特開平10-164349号公報、特開平10-285562号公報、特開平10-334272号公報、特開平10-240626号公報、特開平10-240129号公報（文献4～12）等も、エレクトロニックウォーターマーキング方式に関する発明を開示する。

【0005】しかしながら、これらの文献に開示された方式は、認証情報を埋め込んだ後の画像データの圧縮符号化を十分に考慮していなかった。つまり、これらの方式により埋め込まれた認証情報が量子化値より少ない場合には、埋め込まれた画像データが量子化の結果、消失してしまう可能性がある。

【0006】

【発明が解決しようとする課題】本発明は、上述した従来技術の問題点に鑑みてなされたものであり、圧縮符号化に適した画像処理装置およびその方法を提供することを目的とする。特定的には、本発明は、認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがない画像処理装置およびその方法を提供することを目的とする。

【0007】

【課題を達成するための手段】上記目的を達成するために、本発明にかかる画像処理装置は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換手段と、画像データに対して前記所定の処理を行う処理手段と、前記所定の処理がなされた画像データを量子化処理する量子化手段とを有する。

【0008】好適には、前記処理手段は、前記画像データを分割し、分割した画像データそれぞれに埋め込みデータを埋め込む埋込処理を行い、前記分割された画像データそれぞれに埋め込まれた埋め込みデータを検出する検出手段をさらに有する。

【0009】好適には、前記変換手段は、画像データに含まれる画素それぞれの形式を変換する形式変換手段と、前記量子化処理に用いられる量子化値に基づいて、前記形式が変換された画素データの値を調節処理する調節手段とを有し、前記形式が変換された画素データそれぞれが、前記所定の処理により加わる誤差の値により量子化処理後の値が変化しないようになるまで、前記形式変換処理と、前記調節処理とを繰り返す。

【0010】好適には、前記処理手段は、前記画像データに対して埋込データを埋め込む埋込処理を前記所定の処理として行う。

【0011】好適には、前記処理手段は、所定の鍵情報と前記画像データとに基づいてハッシュ値を計算するハッシュ値計算手段と、計算の結果として得られた前記ハッシュ値を、前記画像データに埋め込む埋込処理手段とを有する。

【0012】好適には、前記画像データに埋め込まれた埋込データを検出する検出手段をさらに有する。

【0013】好適には、前記量子化された画像データを逆量子化する逆量子化手段と、前記逆量子化された画像データに埋め込まれたハッシュ値を抽出する抽出手段と、前記画像データと、前記ハッシュ値の計算に用いられた鍵情報とに基づいて、ハッシュ値を計算する計算手段と、前記抽出されたハッシュ値と前記計算されたハッシュ値とに基づいて、前記量子化された画像データに改ざんが加えられたか否かを検出する改ざん検出手段とを有する。

【0014】また、本発明にかかる画像処理方法は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換し、画像データに対して前記所定の処理を行い、前記所定の処理がなされた画像データを量子化処理する。

【0015】また、本発明にかかる記録媒体は、所定の処理により加わる誤差によって量子化処理後の値が変化しないように画像データの値を変換する変換ステップと、画像データに対して前記所定の処理を行う処理ステップと、前記所定の処理がなされた画像データを量子化処理する量子化ステップとをコンピュータに実行させる

プログラムを記録する。

【0016】

【発明の実施の形態】〔第1実施形態〕以下、本発明の第1実施形態を説明する。

【0017】〔改変判定装置1〕図1は、本発明にかかる画像処理方法を実現する画像処理装置1の構成を示す図である。図1に示すように、画像処理装置1は、CRT表示装置あるいは液晶表示装置等の表示装置100、キーボードおよびマウス等を含む入力装置102、デジタルカメラインターフェースIF（カメラIF）104、メモ리카ードインターフェース（メモ리카ードIF）106、MO装置およびCD装置等の記憶装置108、および、メモリ112およびマイクロプロセッサ（CPU）114等を含むコンピュータ本体（PC本体）110から構成され、必要に応じて、さらに通信装置116が付加される。つまり、画像処理装置1は、一般的なコンピュータに、カメラIF104およびメモ리카ードIF106を付加した構成を採る。

【0018】画像処理装置1は、これらの構成部分により、デジタルカメラ140が撮影した画像データ（JPEG、BMPあるいはYUVなど形式を問わない）を、カメラIF104を介して受け入れる。あるいは、画像処理装置1は、デジタルカメラ140がメモ리카ード142に記録した画像データを、メモ리카ードIF106を介して受け入れる。

【0019】さらに、画像処理装置1は、光磁気ディスク（MO）あるいはコンパクトディスク（CD）等の記録媒体120に記録されて記憶装置108に供給される埋込・検出プログラム2（図2等を参照して後述する）を、メモリ112にロードして実行し、受け入れた画像データに対して、量子化処理しても失われることがないように電子透かし（埋め込みデータ）の埋め込み処理を行う。

【0020】また、画像処理装置1は、埋込・検出プログラム2を実行し、画像データに埋め込まれた電子透かしを検出し、画像データに対して改ざんが加えられたか否か等を判定する。

【0021】〔埋込・検出プログラム2〕まず、埋込・検出プログラム2の構成および動作を説明する。図2は、図1に示した画像処理装置1が実行し、本発明にかかる画像処理方法を実現する埋込・検出プログラム2の構成を示す図である。図2に示すように、埋込・検出プログラム2は、OS80、埋込・抽出部3、鍵情報データベース（DB）22および画像データベース（DB）24から構成される。埋込・抽出部3は、埋込パラメータDB20、制御部26、埋込部30および抽出部40から構成される。

【0022】〔OS80〕OS80は、例えば、OS/2（IBM社）あるいはウィンドウズ（マイクロソフト社）等のオペレーティングシステムソフトウェアであっ

て、埋込・検出プログラム2の各構成部分の実行制御を行う。

【0023】〔制御部26〕埋込・抽出部3の制御部26は、例えば、表示装置100に操作のGUI画像（図示せず）を表示し、表示されたGUI画像に対するユーザの操作を受け入れ、必要に応じて、受け入れた操作を示す操作データを、埋込・検出プログラム2の各構成部分に供給する。また、制御部26は、受け入れたユーザの操作に応じて、埋込・検出プログラム2の各構成部分の動作を制御する。

【0024】〔画像DB24〕画像DB24は、埋込部30が電子透かしを埋め込んだ圧縮画像データ（JPEGデータ）を記憶装置108に挿入された記録媒体120、あるいは、メモ리카ードIF106に挿入されたメモ리카ード142に記憶・管理し、記憶・管理した画像データを読み出して抽出部40に対して出力する。

【0025】〔鍵情報DB22〕鍵情報DB22は、画像DB24が管理するJPEGデータと、埋込部30が、このJPEGデータへ電子透かしを埋め込む際に、乱数を発生させるために用いる鍵（例えば64ビットの数値）とを対応付けた鍵情報を記憶装置108等に記憶・管理し、記憶・管理した鍵情報を読み出して埋込部30および抽出部40に対して出力する。

【0026】〔埋込パラメータDB20〕埋込パラメータDB20は、電子透かしの埋め込み用いるパラメータを記憶・管理し、埋込部30に対して出力する。

【0027】〔埋込部30〕図3は、図2に示した埋込部30の構成を示す図である。図4は、注目DCT係数を示す図である。図3に示すように、埋込部30は、埋込前処理部32、ハッシュ（Hash）値計算部300、ハッシュ値埋込部302および出力フォーマット変換部304から構成される。埋込部30は、これらの構成部分により、まず、各種（JPEG、RGB（ビットマップ（BMP））および輝度・色差（YUV）等）の形式の画像データから、予め定められたハッシュ関数とキーとを用いて、注目するDCT（図4）係数のハッシュ値を計算する。

【0028】さらに、埋込部30は、計算の結果として得たハッシュ値を、画像データ自体に対して電子透かしの手法を用いて埋め込む、あるいは、画像データのヘッダ部分に埋め込む等の方法により、画像データに付加する。なお、埋込部30を画像データのY、U、V各成分から得られたDCT係数に対して、電子透かしの手法を用いてハッシュ値を埋め込むように構成することも、Y、Cr、Cb各成分から得られたDCT係数に対してハッシュ値を埋め込むように構成することも可能であるが、説明の明確化のために、以下、埋込部30が、計算して得たハッシュ値を、画像データのY、U、V各成分から得られたDCT係数に対して埋め込む場合を具体例とする。

【0029】[埋込前処理32]図5は、図3に示した埋込前処理部32の構成を示す図である。また、図5に示すように、埋込パラメータDB20（図2）の埋込前処理32は、フォーマット認識部320、逆量子化部（ $Q^{-1}$ ）322、量子化値計算部324、J P E G' / B M P変換部326、Y U V / B M P変換部328、B M P / J P E G' 変換部330およびD C T係数調整部332から構成される。

【0030】埋込部30は、これらの構成部分により、D C T変換してハッシュ値を埋め込んで電子透かしを埋め込み、さらに、圧縮符号化してJ P E G形式の圧縮画像データ（J P E Gデータ）とした場合であっても、埋め込んだハッシュ値が失われない状態（安定状態）になるように、画像データ（B M Pデータ）に対して埋込前処理を行う。

【0031】[フォーマット認識部320]埋込前処理32において、フォーマット認識部320は、入力された各種形式の画像データ（J P E Gデータ、B M Pデータ、Y U V形式の画像データ（Y U Vデータ）等）のデータフォーマットを識別し、入力された画像データがいずれの形式であるかを判断し、J P E Gデータが入力された場合には、入力されたJ P E Gデータを復号部322に対して出力し、B M Pデータが入力された場合には、入力されたB M PデータをB M P / J P E G' 変換部330に対して出力し、Y U Vデータが入力された場合には、入力されたY U VデータをY U V / B M P変換部328に対して出力する。

【0032】さらに、フォーマット認識部320は、B M Pデータにおいてハッシュ値を埋め込む領域を、例え

$$\begin{aligned} T[X][Y] &= 1 && : (X, Y) \in A \text{ の場合} \\ &= 0 && : (X, Y) \in A \text{ 以外の場合} \end{aligned} \quad (1)$$

【0036】[復号部322] J P E Gデータは、D C T係数に対して量子化処理およびハフマン（Huffman）符号化処理を施すことにより生成される。復号部322は、まず、フォーマット認識部320から入力されたJ P E Gデータをハフマン復号する。また、復号部322は、復号したJ P E GデータのY, U, V各成分からそれらの量子化値 $q[k]$ を計算し、埋込量子化値計算部324に対して出力する。また、復号部322は、計算の結果として得た量子化値 $q[k]$ それぞれを用いて、ハフマン復号したJ P E GデータのY, U, V各成分を逆量子化して、Y, U, V各成分のD C T係数J P E G' を生成し、M C UテーブルTと対応づけてJ P E G' / B M P変換部326に対して出力する。

【0037】[Y U V / B M P変換部328] Y U V / B M P変換部328は、Y U Vデータを、下式2に示す

$$\begin{aligned} R &= (\text{int})(Y + V * 1.4020) \\ G &= (\text{int})(Y - U * 0.3441 - V * 0.7139) \\ B &= (\text{int})(Y + U * 1.7718 - V * 0.0012) \end{aligned}$$

但し、

ば $16 \times 16$ 画素構成のM C U単位で指定する領域指定データAを受け、領域指定データAが示すM C Uそれぞれに含まれるD C T係数が安定状態であるか否かを示すM C UテーブルT（T[X][Y]）、例えば、B M Pデータが $720 \times 480$ 画素構成である場合には $X = 45$ ,  $Y = 30$ ）を作成する。

【0033】なお、領域指定データAにより指定される領域は、J P E G' / B M P変換部326およびY U V / B M P変換部328による変換処理の対象とはならない。画質に与える影響を最小にすることができるという意味で、領域指定データAを、画面の端の領域を指定するように作成すると、そうでない場合に比べてより好適である。フォーマット認識部320は、作成したM C UテーブルTを、J P E Gデータ、B M PデータおよびY U Vデータそれぞれに付して、復号部322、B M P / J P E G' 変換部330およびY U V / B M P変換部328にそれぞれに対して出力する。

【0034】上述のように、M C UテーブルTは、例えば $45 \times 30$ のマトリクス形式で表され、M C UテーブルTの各要素T[X][Y]それぞれは、例えば、対応するM C UのD C T係数データが安定状態である場合には値1、安定でない場合には値0を採る。フォーマット認識部320は、下式1に示すように、M C UテーブルTの初期値として、領域指定データAが示すM C Uに対応するM C UテーブルTの要素T[X][Y]の値を1とし、これら以外のM C Uテーブルの要素T[X]

[Y]の値を0とする。

【0035】

【数1】

ようにB M Pデータ（R G B）に変換し、M C UテーブルTと対応付けてB M P / J P E G' 変換部330に対して出力する。なお、Y U V / B M P変換部328によりY U VデータをB M Pデータに変換する理由は、Y U VデータのY, U, V各成分が、オーバーフローあるいはアンダーフローを起こしていなくても（ $0 \leq Y < 256$ ,  $-128 \leq U, V < 128$ ）、B M Pデータに変換した場合に、B M PデータのR, G, B各成分にオーバーフローあるいはアンダーフローが生じる場合があるので、このような場合においても、最終的に得られるD C T係数を安定状態とすることができるようにするためである。

【0038】

【数2】

$$(2) \quad R = R > 255 ? 255 : R < 0 ? 0 : R$$

$G = G > 255 ? 255 : G < 0 ? 0 : G$

$B = G > 255 ? 255 : B < 0 ? 0 : B$

ここで、 $A = B ? C : D$ は、C codeのものと同じで、

$A = C$  (if B is TRUE)

$A = D$  (if B is NOT TRUE)

である。

【0039】 [J P E G' /B M P変換部326] J P E G' /B M P変換部326は、復号部322およびD C T係数調整部332から入力されるD C T係数J P E G' の内、領域指定データAが示す領域以外のMCUのY, U, V成分それぞれのD C T係数を逆D C T (I D C T) 処理する。J P E G' /B M P変換部326は、さらに、I D C T処理の結果として選ばれたY, U, V成分を、Y U V /B M P変換部328と同様に上記式2に従ってB M Pデータに変換し、MCUテーブルTと対応づけてB M P /J P E G' 変換部330に対して出力する。

【0040】 [B M P /J P E G' 変換部330] B M

$Y = R * 0.2990 + G * 0.5870 + B * 0.1140$

$U = -R * 0.1684 - G * 0.3316 + B * 0.5000$

$V = R * 0.5000 - G * 0.4187 - B * 0.0813$

【0042】 [埋込量子化値計算部324] 埋込量子化値計算部324は、領域指定データAにより示されるD C T係数 (注目D C T係数)  $d c t\_c o e f f i$  の埋込量子化値 $q\_e m b [k]$ を算出する。さらに埋込量子化値計算部324の処理を詳細に説明する。埋込量子化値計算部324は、注目D C T係数 $d c t\_c o e f f i$  およびデコーダ最大計算誤差 $\delta$ を、埋込パラメータD B 20 (図2) から受ける。

【0043】 [注目D C T係数 $d c t\_c o e f f i$ ] ここでは、注目D C T係数 $d c t\_c o e f f i$ を詳細に説明する。注目D C T係数 $d c t\_c o e f f i$ は、

電子透かしの埋め込みに用いる $8 \times 8$ 画素構成のD C Tブロックに含まれる1つ以上のD C T係数であり、Y, U, V成分のいずれのD C T係数であってもよいが、以下、説明の明確化のために、注目D C T係数 $d c t\_c o e f f i$ としてY成分のD C T係数の内の直流成分 $d c t\_c o e f f i (0, 0)$ を用い、ハッシュ値の埋め込みのために、同じくY成分のD C T係数の内の $(1, 1), (1, 2), (2, 1), (2, 2)$ を利用する場合を具体例とする。

【0044】 [デコーダ最大計算誤差 $\delta$ ] ここでは、デコーダ最大計算誤差 $\delta$ を詳細に説明する。また、ハッシュ値を埋め込んだJ P E Gデータを伸長復号処理するデコーダが違う場合には、システム間でI D C T処理の結果に誤差が生じる可能性がある。デコーダ最大計算誤差 $\delta$ は、埋め込み量子化値:システム(decoder)の違いから生じるI D C T処理の誤差の2倍の値に設定される。な

$$q\_emb[k] = (\text{int}((\delta - 1) / q[k] + 1) * q[k]) \quad (4)$$

【0048】 なお、量子化値 $q [k]$ がデコーダ最大計

P /J P E G' 変換部330は、J P E G' /B M P変換部326、フォーマット認識部320またはY U V /B M P変換部328から入力されるB M Pデータの内、同じくこれから入力されるMCUテーブルTの値0の要素T [X] [Y] (T [X] [Y] = 0)に対応するMCUに含まれるB M PデータのR, G, B成分それぞれを、下式3に示すように、Y, U, V各成分に変換し、さらに、変換の結果として選ばれたY, U, V各成分を、 $8 \times 8$ 構成のD C TブロックごとにD C T処理してD C T係数J P E G' を生成する。つまり、B M P /J P E G' 変換部330は、入力されるB M Pデータの内、まだ安定状態になっていないB M PデータをD C T係数J P E G' に変換する。B M P /J P E G' 変換部330は、変換処理の結果として得られたD C T係数J P E G' を、MCUテーブルTと対応づけてD C T係数調整部332に対して出力する。

【0041】

【数3】

(3)

お、I D C T処理の誤差は、ほとんどの場合、2以下である。従って、デコーダ最大計算誤差 $\delta$ の設定値は4以上あれば充分である。以下、デコーダ最大計算誤差 $\delta$ の値を、十分に大きい12に設定する場合を具体例として説明する。

【0045】 埋込量子化値計算部324は、埋込前処理32に入力された画像データがJ P E Gデータである場合には、復号部322から入力された量子化値 $q [k]$ を、J P E Gデータでない場合には、例えば、入力装置102を介してユーザが入力する量子化値 $q [k]$ を用いて以下の処理を行う。なお、埋込量子化値計算部324は、例えば、埋込前処理32に入力された画像データがJ P E Gデータでなく、しかも、入力装置102から量子化値 $q [k]$ の入力がない場合には、量子化値 $q [k]$ の全ての要素の値をデコーダ最大計算誤差 $\delta$ に設定する ( $q [k] = \delta$ )。

【0046】 次に、埋込量子化値計算部324は、領域指定データAが示す注目D C T係数 $d c t\_c o e f f i$ それぞれに対応する埋込量子化値 $q\_emb [k]$  ( $k \in \{d c t\_c o e f f i\}$ ) を、下式4に示すように計算する。なお、埋込量子化値 $q\_emb [k]$ は、ハッシュ値を埋め込んだD C T係数を量子化処理するために用いられる量子化値であって、量子化値 $q [k]$ の整数倍の値を採る。

【0047】

【数4】

算誤差 $\delta$ よりも大きい場合 ( $q [k] \geq \delta$ )、埋込量子

化値  $q\_emb[k]$  と量子化値  $q[k]$  とは一致する ( $q\_emb[k] = q[k]$ )。また、埋込前処理 3 2 に J P E G データが入力される場合、量子化値  $q[k]$  の変更は不要である。

【0049】 D C T 係数調整部 3 3 2 D C T 係数調整部 3 3 2 は、J P E G' / B M P 変換部 3 2 6、B M P / J P E G' 変換部 3 3 0 および D C T 係数調整部 3 3 2 により構成されるループ処理を制御し、このループ処理を所定の回数 (例えば 5 回) 繰り返して、B M P / J P E G' 変換部 3 3 0 から入力された注目 D C T 係数  $dct\_coeffi$  が、埋込量子化値  $q\_emb[k]$  の整数倍に近い値をとるように、つまり、注目 D C T 係数  $dct\_coeffi$  が安定状態になるようにそれらの値を調整する。

【0050】以下、さらに D C T 係数調整部 3 3 2 の処理を詳細に説明する。D C T 係数調整部 3 3 2 は、埋込パラメータ D B 2 0 (図 2) から安定化閾値  $\Delta$  を受け

$$|c[k] - coeff\_emb[k] * q\_emb[k]| < \Delta / 2 \quad (5)$$

【0053】 D C T 係数調整部 3 3 2 は、全ての M C U の全ての D C T ブロックに含まれる D C T 係数が式 5 を満し、安定状態になっている場合には、注目 D C T 係数  $dct\_coeffi$  およびその他の D C T 係数を画像 D B 2 4 (図 2) に対して出力し、安定状態になっていない場合には、安定状態になっていない D C T 係数が安定状態になるように調節する。なお、D C T 係数調整部 3 3 2 は、 $coeff\_emb[k]$  を、領域指定データ A が示す注目 D C T 係数  $dct\_coeffi$  として、それ以外の D C T 係数は、量子化処理した値 ( $coeff\_emb[k] = coeff\_emb[k] * q\_emb[k]$  : if  $k \in \{dct\_coeffi\}$ )

$$c[k] = (int)(c[k] > 0 ? c[k] / q[k] + \alpha : c[k] < 0 ? c[k] / q[k] - \alpha : 0) * q[k] \quad otherwise$$

$$coeff\_emb[k] = (int)(c[k] > 0 ? c[k] / q\_emb[k] + \alpha : c[k] < 0 ? c[k] / q\_emb[k] - \alpha : 0) \quad (6)$$

【0056】式 6 において、 $\alpha$  は 0 ~ 0.5 の間の値を採る数値であって ( $0 \leq \alpha \leq 0.5$ )、 $\alpha$  の値を大きくすると、安定化処理が再生画像に与える変化を小さくすることができる。しかしながら、変換後の  $coeff[k]$  の値の絶対値は常に大きくなり、安定状態にした後の D C T 係数を変換して得られる B M P データの R、G、B 成分の値に近づくので、B M P データの R、G、B 成分の値にオーバーフロー・アンダーフローが生じやすい。一方、 $\alpha$  を小さくすると、変換後の  $coeff[k]$  の値の絶対値は常に小さくなり、安定状態にした後の D C T 係数を変換して得られる B M P データの R、G、B 成分それぞれの値は 128 に近づくので、B M P データの R、G、B 成分の値にオーバーフロー・アンダーフローが生じにくい。

【0057】このような  $\alpha$  の性質を考慮し、安定化処理

る。安定化閾値  $\Delta$  は、注目 D C T 係数  $dct\_coeffi$  が、埋込量子化値  $q\_emb[k]$  の整数倍に近い値になっているか否かを判断するために用いられる閾値であって、例えばデコーダ最大計算誤差  $\delta$  よりも小さい値、例えば 1 程度の値に設定される ( $\delta > \Delta = 1.0$ )。

【0051】 D C T 係数調整部 3 3 2 は、次に、領域指定データ A により示される M C U の D C T ブロックそれぞれに含まれる各 D C T 係数が、下式 5 を満たしているか否かを判断する。D C T 係数調整部 3 3 2 は、判断対象の D C T ブロックに含まれる D C T 係数のすべてが下式 5 を満たしている場合には、この D C T ブロックに対応する M C U テーブル T の要素 T [X] [Y] の値を安定状態を示す 1 とし (T [X] [Y] = 1)、これ以外の場合には 0 とする (T [X] [Y] = 0)。

【0052】

【数 5】

$coeffi[k] = c[k] / q[k]$  を、画像 D B 2 4 (図 2) に対して出力する。

【0054】 D C T 係数の安定化 ここでは、D C T 係数調整部 3 3 2 が D C T 係数を安定状態にする処理 (安定化処理) を詳細に説明する。D C T 係数調整部 3 3 2 は、値が 0 の M C U テーブル T の要素 T [X] [Y] に対応する M C U の D C T 係数を、下式 6 に示すように変換する。

【0055】

【数 6】

が再生画像に与える影響を極力少なくし、かつ、安定化した D C T 係数を変換して得られる B M P データにオーバーフロー・アンダーフローが生じないようにするために、D C T 係数調整部 3 3 2 は、J P E G' / B M P 変換部 3 2 6、B M P / J P E G' 変換部 3 3 0 および D C T 係数調整部 3 3 2 によるループ処理を 1 回行うごとに、 $\alpha$  の値を減らしてゆくようにする。

【0058】例えば、J P E G' / B M P 変換部 3 2 6、B M P / J P E G' 変換部 3 3 0 および D C T 係数調整部 3 3 2 によるループ処理の回数を  $loopcount$  とすると、D C T 係数調整部 3 3 2 は、下式 7 に示すように、ループ処理の回数に応じて  $\alpha$  の値を少なくする。

【0059】

【数 7】



$$\alpha = \begin{cases} 0.5 \text{loopcount}/10 & (\text{loopcount} < 5) \\ 0 & (\text{loopcount} \geq 5) \end{cases} \quad (7)$$

【0060】DCT係数調整部332は、上述した調整を、値が0のMCUテーブルTの要素T[X][Y]に対応するMCUに含まれるDCTブロック全てのDCT係数に対して行い、JPEG' /BMP変換部326に対して出力する。

【0061】なお、ごくまれに、JPEG' /BMP変換部326における処理でオーバーフロー・アンダーフローが生じていて、ループ処理を5回繰り返した後でも、式5の条件を満たすことがないDCT係数が存在することがある。このような場合に対応するために、DCT係数調整部332は、ループ処理を5回繰り返した後は、さらに、DCT係数の値が式5の条件を満たすようになるまでループ処理を1回ずつ追加して行い、ループ処理を1回追加するたびに、coeff\_emb[k]の絶対値を1（但し、何らかの制約がある場合、その制約を満たす1以上の最小数）ずつ減らす。このように、ループ処理を追加し、ループ処理1回ごとにcoeff\_emb[k]の絶対値を1（但し、何らかの制約がある場合、その制約を満たす1以上の最小数）ずつ減らすことにより、DCT係数調整部332は、画像の変化を極力少なくしつつ、ループ処理を有限回数に抑える。

【0062】以上説明した埋込前処理32の処理により、図6(A)に示すように分布していた注目DCT係数dct\_coeffiの値は、図6(B)に示すように、埋込量子化値q\_emb[k]の整数倍に近い値を

$$\text{err}[k] = |c2[k] - \text{coeff\_emb}[k] * q\_emb[k]| > q\_emb[k]/2 (> \delta/2) \quad (8)$$

【0065】例えば、あるBMPエンコーダでiDCT処理結果(iDCTデータ)あるいはYUVデータをBMPデータに変換する処理を小数点第1位まで用いて計算する際に、iDCTデータの計算誤差が最悪0.05あり、iDCT処理で、係数1つにつき64回の加算または減算を行うとすると、計算誤差は最悪3.35(=0.05×63+3)となるが、上述したように、最大誤差δを12より大きい値にとれば、上述した式8を満たすことはない。

【0066】逆に、iDCT等の計算で少数第1位以上の誤差があるようなシステムは、誤差が大きすぎて、単なる変換だけで画像が大きく変化してしまい、使用に耐えないシステムと言える。多数のシステムを調べると、最悪でerr[k]=3.0程度である。よって、全ての{dct\_coeffi}に対して全てのq\_emb[k]による量子化値coeff\_emb[k]は、JPEGデータをBMPデータに変換する処理に耐えられることになる。そのため、coeff\_emb[k]のハッシュ値を取り、その結果をJPEGデータのヘッダ部分に書き込むか、画像自体に電子透かしで埋めておけば良い。

【0067】埋込みに使われる領域Aを除き、鍵DBからえられる、埋込み者、検出者で共通の鍵Kを使い、

採るようになり、埋込量子化値q\_emb[k]の整数倍を中心とする広がりσ(σ<δ)の範囲内に分布するようになる。

【0063】[ハッシュ値計算部300]再び図3を参照する。以上説明した埋込前処理32(図3、4)の処理により、{dct\_coeffi}の全てのDCT係数が埋込みの量子化値q\_emb[k]の整数倍の近傍に来て安定化している。即ち、上述した式5を満たしている。問題は、埋込前処理32の出力から得られるJPEGデータを、JPEG' /BMP変換部326(図5)以外BMPエンコーダにより処理して式5に示した性質が保てるか否かである。例えば、埋込前処理32

(図3、4)の出力データをinput.bmp、え44以外のエンコーダで作られるBMPデータをinput2.bmpとすると、これらの違いは、JPEGデータをiDCTし、さらにYUVデータに変換し、これをBMPデータに変換する処理における計算の誤差であり、この誤差のために、2つのinput.bmpとinput2.bmpとが、下式8に示すように、量子化値を跨いでしまう可能性が高い。即ち、input.bmpから導かれたDCT係数c2[k]が、下式8を満たす可能性は小さい。

【0064】

【数8】

ハッシュ値DCT\_hashを、下式9に示すように計算する。

【0068】

【数9】

$$\text{DCT\_hash} = \text{hash}(K, \text{coeff\_emb}[k]) \quad (9)$$

【0069】なお、式9におけるhash( )としては、MD5などがある。また、鍵Kとしては、64ビット鍵、DCT\_hashは64ビット長が妥当な長さである。

【0070】[ハッシュ値埋込部302]ハッシュ値埋込部302は、ハッシュ値計算部300で選られたDCT\_hashを画像に埋め込む。画像に埋め込むアルゴリズムは何を用いてもよいが、画像を痛めない方法としてはLSB法がよい。LSB法とは、電子透かしをデジタルコンテンツに埋め込む方式の1つで、コンテンツの特微量のLSB(least significant bit、最下位bit)をある規則に従って変化させることによって、情報を埋め込む。LSBを変化させる理由は、埋込み後のデジタルコンテンツ(画像、音)の変化が殆ど無い為である。

【0071】以下、具体例を挙げて説明する。埋込パラメータDB20(図2)から得られる埋込みに利用するDCT係数{dct\_coeffi}の要素がn個あ

り、hash\_embが64ビットで、1つのサブブロック(8×8画素)にmビットを埋め込む事を考える( $n \geq m$ )。つまり、埋め込みに64/m個のサブブロックが必要となる。

【0072】ここで、埋め込みによる画質の痛みを極力防ぐ為に、Aの候補を予め幾つか決めておいて(例：画面の上、下、右、左端の4箇所)、そのどこかに埋めて、検出時に全て試すという方法もある。さて、ここで、{dct\_coeff\_i}のLSBに埋めたいbitを埋めていくわけである。

【0073】

【数10】

$emb\_coeff[k] = 2p + emb\_bit[k] \quad (10)$

pはある整数、emb\_bit[k]は係数kに埋めたいbit, 0 or 1

【0074】上式10を満たすようにemb\_coeff[k]を変更後、Aの領域のみのDCT係数をJPEG'/BMP変換部326(図5)に入力し、A内の全ての{dct\_coeff\_i}のDCT係数が、上式10を満たしつつ安定になるようにすれば良い。この場合、常に、emb\_coeff[k]の値の絶対値が大きくなり方向に変更していれば、つまり $\alpha$ を小さく取れば、収束は速く、式6が達成できる。式6が達成出来れば、Aは安定の為、BMPデータに変換した後も、埋めたビットが変化しない。

【0075】[出力フォーマット変換部304]出力フォーマット変換部304は、ハッシュ値埋込部302の出力結果に対して量子化処理などを行い、入力装置102(図1)を介して設定されるユーザ所望の出力フォーマットに変換する。出力フォーマットがJPEGの際、{dct\_coeff\_i}に属するDCT係数も、q\_emb[k]ではなく、q[k]で量子化する。q[k]で量子化された値coeff[k]は、emb\_coeff[k], q[k], q\_emb[k]より、 $coeff[k] = emb\_coeff[k] * q\_emb[k] / q[k]$ によって計算される。

【0076】[検出部40]以下、検出部40(図2)を説明する。埋め込み装置で埋め込まれた画像データを入力し、鍵Kより注目するDCT成分のハッシュ値を計算し、領域Aに埋め込まれているハッシュ値と比較し、画像自体が改ざんされたかどうかを検出する。

【0077】[検出前処理部42]図7は、図2に示した検出部40の構成を示す図である。図8は、図7に示した検出前処理部42の構成を示す図である。検出部40において、検出前処理部42は、入力画像より埋め込み量子化値q\_emb[k]を逆算する。

【0078】[フォーマット認識部420]フォーマット認識部420は、入力画像のフォーマットを認識し、JPEGなら復号部422に対して出力し、BMP, YUVならBMP, YUV/JPEG'変換部424に対

して出力する。

【0079】[復号部422]復号部422は、入力画像を復号し、Aを除く画像全体の注目するDCT成分の係数を逆量子化して、JPEG'画像とする。

【0080】[BMP, YUV/JPEG'変換部424]BMP, YUV/JPEG'変換部424は、入力されたBMP, YUVデータをDCT処理し、JPEG'データに変換する。

【0081】[量子化値逆算部426]

【0082】図9および図10は、図8に示した量子化値逆算部426における埋め込み量子化値逆算処理を示す第1および第2のフローチャートである。量子化値逆算部426は、復号部422およびBMP, YUV/JPEG'変換部424の出力の注目するDCT成分 $k \in \{dct\_coeff\_i\}$ の画像全体での絶対値の最大係数をmax[k]として、各々の仮定した量子化値iの回りにどのくらいDCT係数が集まっているかのヒストグラムから示すように計算する。図9に示すように、フォーマット認識部420への入力フォーマットがJPEGの場合、 $i = q[k] * n$  ( $n = 1, 2, \dots$ ) に対してのみ調べれば良い。

【0083】図9に示した処理により求められたヒストグラム[i]の最大値を与えるiを、max\_iとおき、図10に示した処理にしたがって、q\_emb[k]を決定する。図10では、図9でq\_emb[k]が、max\_iの倍数であることからq\_emb[k]を求めている。

【0084】ここで、T\_threは1より少し小さい値で、T\_thre=0.8辺りが妥当である。ここで、T\_threの値の精度等より図9および図10に示した処理によりうまくq\_emb[k]が求められない例外的な画像に関して、埋め込み処理の過程において、図9および図10に示した処理により、正しくq\_emb[k]が満たされるようなヒストグラムになるようにすればよい。例えば、q\_emb[k]\*2nの周りに多く係数が集まってしまうような場合、画像全体のうち、痛みが少なそうなところで、q\_emb[k]\*2n+1に埋め込むようにすれば良い。

【0085】[ハッシュ値抽出部400]再び図7を参照する。ハッシュ値抽出400は、埋め込み領域Aにおいて、埋込パラメータDB20からの埋め込みDCT成分{dct\_coeff\_i}の係数c[k]と、検出前処理部42によって計算された、埋め込み量子化値q\_emb[k]より、以下の方法でLSBをしらべ、それらを並べて埋め込まれたハッシュ値embed\_hashを計算する。

【0086】

【数11】

$$LSB = (int)((c[k] + \beta) / q\_emb[k]) \bmod 2$$

$$\text{但し、} \beta = c[k] > 0 ? q\_emb[k]/2 : -q\_emb[k]/2 \quad (11)$$

【0087】 [ハッシュ値計算部402] ハッシュ値計算部402は、A以外の領域に対して、{dct\_coeffi}の係数C[k] q\_emb[k]より、上記式6において $\alpha=0.5$ として、coeff\_emb[k]を求め、上記式9によりDCT\_hashを計算する。

【0088】 [改ざん検出部404] 改ざん検出部404は、ハッシュ値抽出400およびハッシュ値計算部402から得られるDCT\_hash, embed\_hashが、DCT\_hash==embed\_hashなら改ざんなし、それ以外の場合(DCT\_hash≠embed\_hash)には改ざん有りとして、表示装置100(図1)等に表示する。

【0089】 [全体動作] 図11は、埋込・検出プログラム2(図2)による埋め込み処理を示すフローチャートである。図12は、埋込・検出プログラム2(図2)による検出処理を示すフローチャートである。なお、図11および図12の各処理中の括弧内の番号は、その処理を行う埋込・検出プログラム2の構成部分(図3, 5, 7, 8)に付された符号を示す。埋込・検出プログラム2の各構成部分は、図11に示すように埋め込み処理を行い、図12に示すように検出処理を行う。

【0090】 [変形例] 以下、本発明に係る埋め込み装置の変形例を説明する。図13は、埋込・検出プログラム2(図2)において埋込部30の代わりに用いられる埋込部50の構成を示す図である。図14は、図13に示した埋込前処理部52の構成を示す図である。図15は、図13に示した改ざんマーク埋込部54の構成を示す図である。

$$R = \text{LFSRb}(K, R0)$$

【0096】 [合成部544] 合成部544は、データを埋め込む場合に、埋め込みデータとRより埋め込みbit列R'を合成して作成する。なお、合成部544が、改ざんマークを埋め込む場合、R'=Rとなる。データを埋め込む場合は、下式13により示されるR'が埋め込みbitになる。ここで、^はxorを意味する。但し、dataは540

$$R' = R \wedge data$$

【0098】 [LSB操作部546] LSB操作部546は、R'とq\_emb[k], c[k], k, (x, y)より、{dct\_coeffi}に属するDCT係数のLSBを操作する。まず、埋め込みビットemb\_bit[k]は、下式14を埋め、あとは、上記式10

$$emb\_bit[k] = (R' > (xn+90yn+1)) \& 1$$

【0100】 [DCT成分分割部528] DCT成分分割部528は、復号部522およびBMP, YUV/JPEG'変換部524から入力されるDCT係数(量子化されていない)を注目DCT({dct\_coeffi})とそうでないものに分ける。

【0101】 [量子化値計算部526] 量子化値計算部

【0091】 なお、埋込部50の構成部分の内、出力フォーマット変換部502は、埋込部30(図3)の出力フォーマット変換部304に同じであり、埋込前処理部52の構成部分の内、フォーマット認識部520、復号部522、BMP, YUV/JPEG'変換部524、量子化値変換部526および量子化値計算部526は、それぞれ埋込前処理32(図5)のフォーマット認識部320、復号部322、JPEG'/BMP変換部326、YUV/BMP変換部328および埋込量子化値計算部324に同じである。また、埋込部50においては領域Aは存在しない。

【0092】 [埋め込み前処理部52] 埋込前処理部52は、入力画像より、DCT係数を抽出する。

【0093】 [改ざんマーク埋め込み部54] 改ざんマーク埋込部54は、改ざんマークあるいはデータを埋め込む部分で、埋め込みアルゴリズムは何でも良く、画像を痛めない方法としてはLSB法がある。

【0094】 [画像分割部540] 画像を8×8画素のブロック(イントラブロック)単位に分割し、入力注目DCT成分l, 係数c[k]と画像位置(x, y)を出力する。

【0095】 [乱数発生部542] 乱数発生部542は、鍵Kより乱数Rを発生させる。Rは、埋め込みに必要なbit数だけのbitが必要で、720x480画素の場合、90x60xn=5400n bit以上である必要がある。Rの作成方法は色々あるが、LFSRを使う場合、b=(int)(1+log25400n)bitのLFSRを使って、Kをkey, R0を鍵DBより得られる初期値(鍵の1部と考えても良い)、LFSRbをb bitのLFSR計算部として、下式12により求められる。

【数12】

$$(12)$$

0n bitの埋め込みdataで、埋め込みたいdataがm bitで、m<5400n bitの場合、埋め込みdataをm周期で繰り返して、5400n/m回繰り返して埋める、等の方法もある。

【0097】

【数13】

$$(13)$$

を満たすように、{dct\_coeffi}に属する全てのDCT係数をT[x][y]=0を満たす全てのMCUに対して行う。

【0099】

【数14】

$$(14)$$

526は、上述したように埋込量子化値計算部324と同じである。但し、T[45][60]を、初期状態(T[x][y]=0, for all x, y)で出力する。

【0102】 図16は、図15に示した埋込後処理部56の構成を示す図である。なお、埋込後処理部56の構

成部分の内、DCT係数調整564は、埋込前処理32のDCT係数調整部332(図5)と同じである。

【0103】[JPEG' /BMP変換部560] JPEG' /BMP変換部560は、入力されたJPEG'画像をiDCT変換して、オーバーフロー/アンダーフロー処理をして、BMPフォーマットの画像に変換する。

【0104】[BMP / JPEG' 変換部562] BMP / JPEG' 変換部600は、入力BMP画像をDCT変換し、JPEG' フォーマットの画像に変換する。

【0105】図17は、埋込・検出プログラム2(図2)において、検出部40の代わりに用いられる検出部60の構成を示す図である。検出部60は、図13~16に示した検出部40により埋め込まれた画像データが、データ埋め込みでなく、改ざんマークを埋め込みである場合、その画像の改ざんの有無を検出し、改ざん場所を8×8画素のブロック単位で特定する。{dct\_coef}の要素がn個ある場合、各々の8×6画素構成のブロック(イントラブロック)の改ざん検出率は1-2<sup>-n</sup>であり、本発明例の様にn=4の場合、その確率は93.75%である。

【0106】[検出前処理部600] 検出前処理部600は、図7に示した検出前処理部42と同じである。但し、埋込領域Aはない。

$$x = (\text{int})(p/n) \bmod 90$$
$$y = (\text{int})(p/n/90)$$

【0111】[出力フォーマット変換部608] 出力フォーマット変換部608は、画像DB24より入力した画像を、改ざん場所がわかるように変化させて出力する。

【0112】[全体動作] 図18および図19は、検出部40および検出部60の処理を示すフローチャートであり、図中の括弧内の番号は、各処理を行う構成部分の符号を示す。検出部40および検出部60は、図18に示すように埋め込み処理を行い、図19に示すように検出処理を行う。

【0113】

【発明の効果】 上述したように、本発明にかかる画像処理装置およびその方法は、圧縮符号化に適している。特定的には、本発明にかかる画像処理装置およびその方法によれば、認証情報を埋め込んだ後に量子化処理をしても、埋め込まれた認証情報が失われることがない。

【図面の簡単な説明】

【図1】 本発明にかかる画像処理方法を実現する画像処理装置の構成を示す図である。

【図2】 図1に示した画像処理装置が実行し、本発明にかかる画像処理方法を実現する埋込・検出プログラムの構成を示す図である。

【図3】 図2に示した埋込部の構成を示す図である。

【図4】 注目DCT係数を示す図である。

【0107】[埋め込みデータ抽出部602] 埋込データ抽出部602は、{dct\_coef}の要素のDCT係数のLSBを抽出し、埋め込みデータを抽出する。イントラロケーション(x, y) (0<=x<60, 0<=y<90), {dct\_coef}の要素数nのLSBを式11により計算し、それを(xn+90yn+1)bit目に持つ5400nbitの抽出データembed\_dataを計算する。

【0108】[埋め込みデータ計算部604] 埋込データ計算部604は、図15に示した乱数発生部542および合成部544と同じ方法で、埋め込みbit列R'を計算する。

【0109】[改ざん検出・場所特定部606] 改ざん検出場所特定部606は、embed\_data, R'から入力画像に改ざんがあったかどうか、あった場合、何処が改ざんされたかを特定する。つまり、改ざん検出場所特定部606は、embed\_data=R'の場合、改ざんなしと判定し、これ以外の場合(embed\_data<>R')には、ビット単位で値が合わない部分を全て探す。その際、例えば、pbit目(0 origin)が合わない場合、改ざんのあったintra location (x, y)は、以下の式によって特定出来る。

【0110】

【数15】

(15)

【図5】 図3に示した埋込前処理部の構成を示す図である。

【図6】 (A)は、図3に示した埋込前処理による安定化処理の前の注目DCT係数dct\_coefの値の頻度をq[k]=3, q\_emb[k]の場合について例示し、(B)は埋込前処理による安定化処理の後の注目DCT係数dct\_coefの値の頻度を同様に例示するヒストグラムである。

【図7】 図2に示した検出部の構成を示す図である。

【図8】 図7に示した検出前処理部の構成を示す図である。

【図9】 図8に示した量子化値逆算部における処理を示す第1のフローチャートである。

【図10】 図8に示した量子化値逆算部における処理を示す第2のフローチャートである。

【図11】 埋込・検出プログラム(図2)による埋め込み処理を示すフローチャートである。

【図12】 埋込・検出プログラム(図2)による検出処理を示すフローチャートである。

【図13】 埋込・検出プログラム(図2)において埋込部の代わりに用いられる埋込部の構成を示す図である。

【図14】 図13に示した埋込前処理部の構成を示す図である。

【図15】 図13に示した改ざんマーク埋込部の構成を

示す図である。

【図 1 6】図 1 5 に示した埋込後処理部の構成を示す図である。

【図 1 7】埋込・検出プログラム（図 2）において用いられる第 2 の検出部の構成を示す図である。

【図 1 8】検出部および検出部（図 1 3 ～ 1 7）の処理を示す第 1 のフローチャートである。

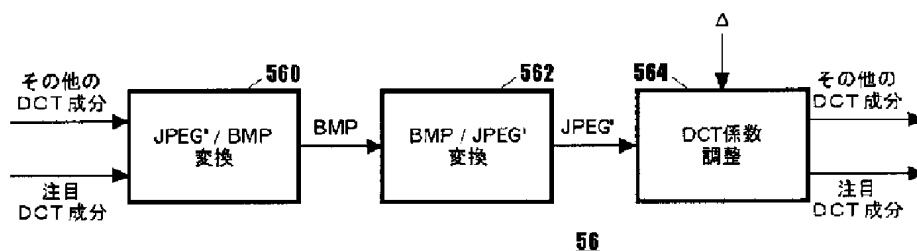
【図 1 9】検出部および検出部（図 1 3 ～ 1 7）の処理を示す第 2 のフローチャートである。

【符号の説明】

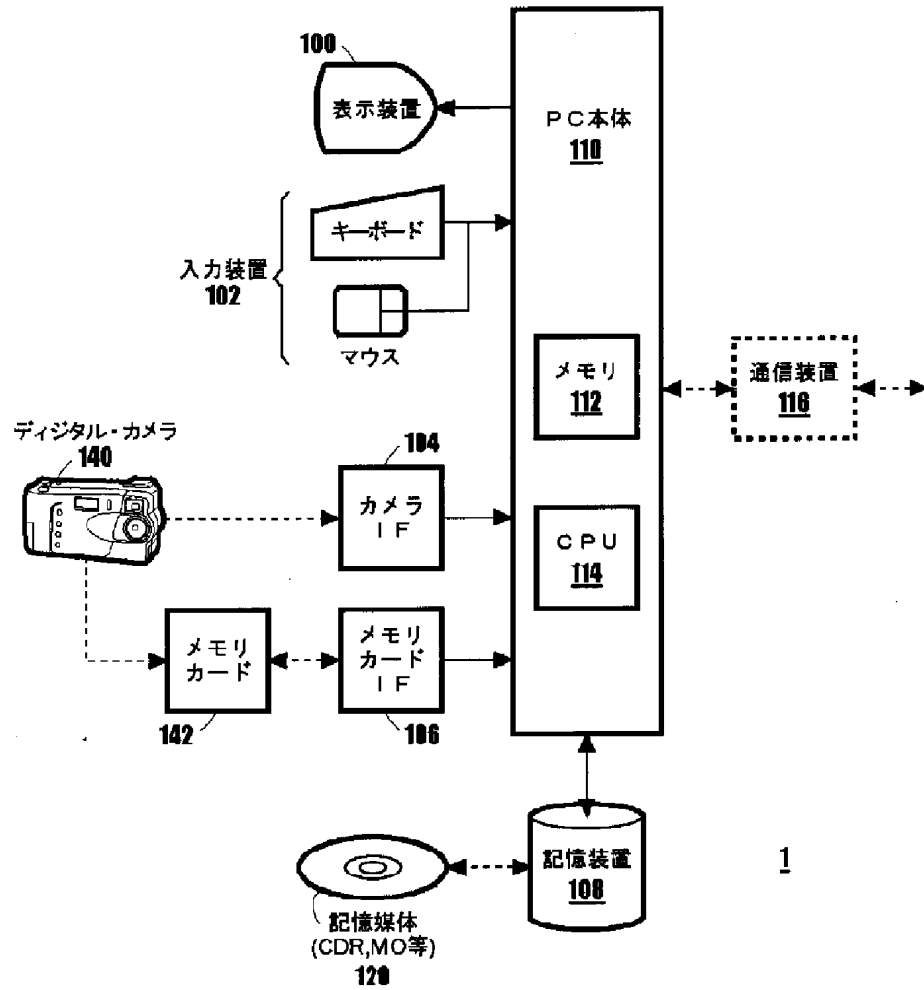
1・・・画像処理装置  
100・・・表示装置  
102・・・入力装置  
104・・・カメラ I F  
106・・・メモリカード I F  
108・・・記憶装置  
110・・・P C 本体  
112・・・メモリ  
114・・・C P U  
116・・・通信装置  
120・・・記録媒体  
140・・・デジタルカメラ  
142・・・メモリカード  
2・・・埋込・検出プログラム  
20・・・埋込パラメータ D B  
22・・・鍵情報 D B  
24・・・画像 D B  
26・・・制御部  
30・・・埋込部  
32・・・埋込前処理  
320・・・フォーマット認識部  
322・・・復号部  
324・・・埋込量子化値計算部  
326・・・J P E G' / B M P 変換部  
328・・・Y U V / B M P 変換部  
330・・・B M P / J P E G' 変換部  
332・・・D C T 係数調整部

300・・・ハッシュ値計算部  
302・・・ハッシュ値埋込部  
304・・・出力フォーマット変換部  
40・・・検出部  
42・・・検出前処理部  
420・・・フォーマット認識部  
422・・・復号部  
424・・・B M P, Y U V / J P E G' 変換部  
426・・・量子化値逆算部  
400・・・ハッシュ値抽出部  
402・・・ハッシュ値計算部  
404・・・改ざん検出部  
50・・・埋込部  
52・・・埋込前処理部  
520・・・フォーマット認識部  
522・・・復号部  
524・・・B M P, Y U V / J P E G' 変換部  
526・・・量子化値計算部  
528・・・D C T 成分分割部  
54・・・改ざんマーク埋込部  
540・・・画像分割部  
542・・・乱数発生部  
544・・・合成部  
546・・・L S B 操作部  
56・・・埋込後処理部  
560・・・J P E G' / B M P 変換部  
562・・・B M P / J P E G' 変換部  
564・・・D C T 係数調整部  
502・・・出力フォーマット変換部  
60・・・検出部  
600・・・検出前処理部  
602・・・埋込データ抽出部  
604・・・埋込データ計算部  
606・・・改ざん検出場所特定部  
608・・・出力フォーマット変換部  
80・・・O S

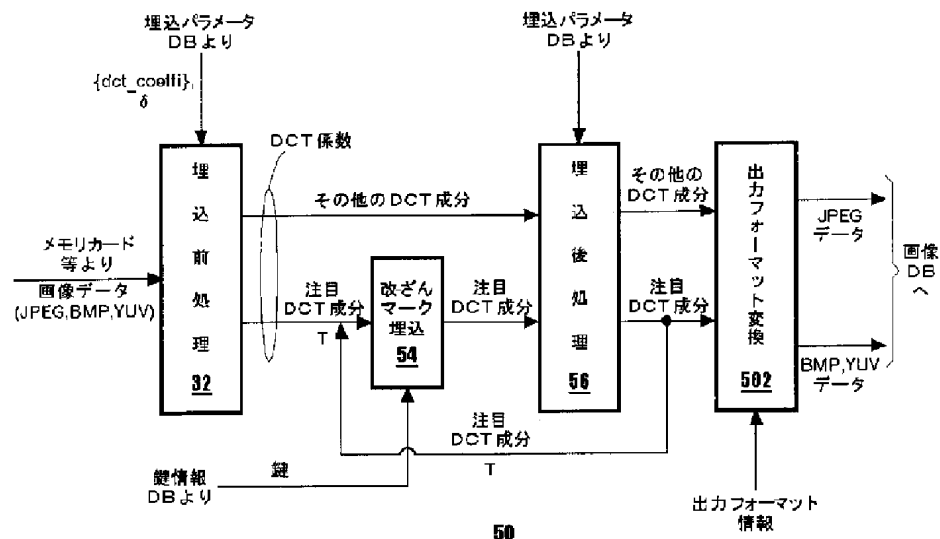
【図 1 6】



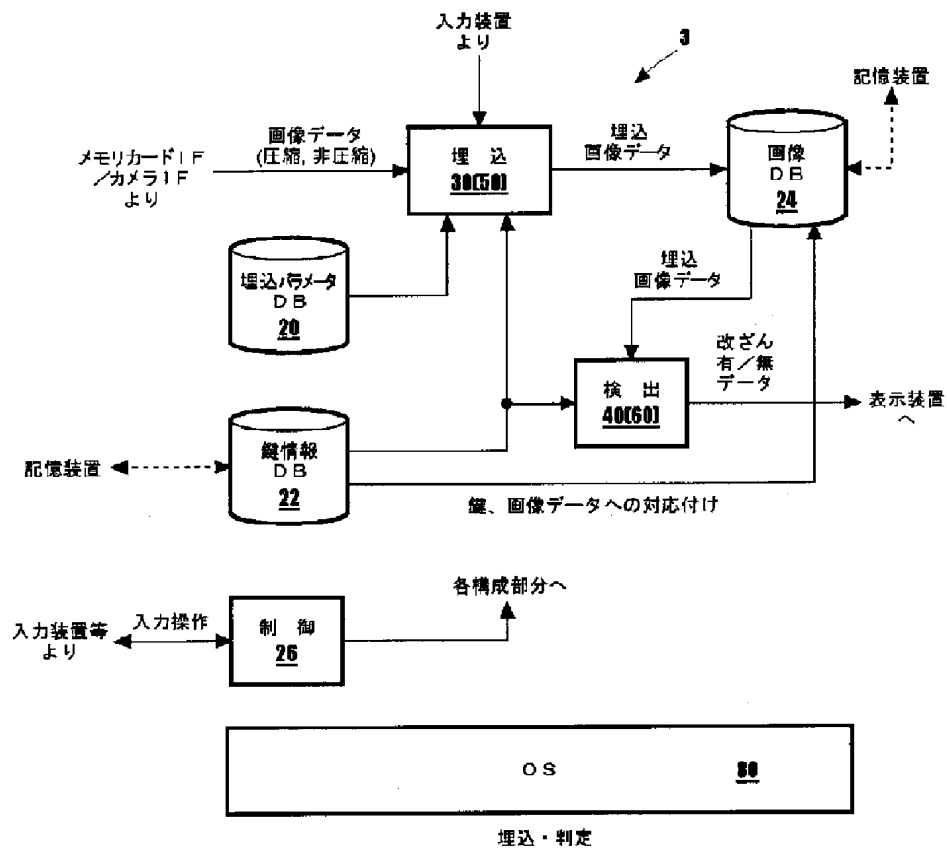
【図1】



【図13】

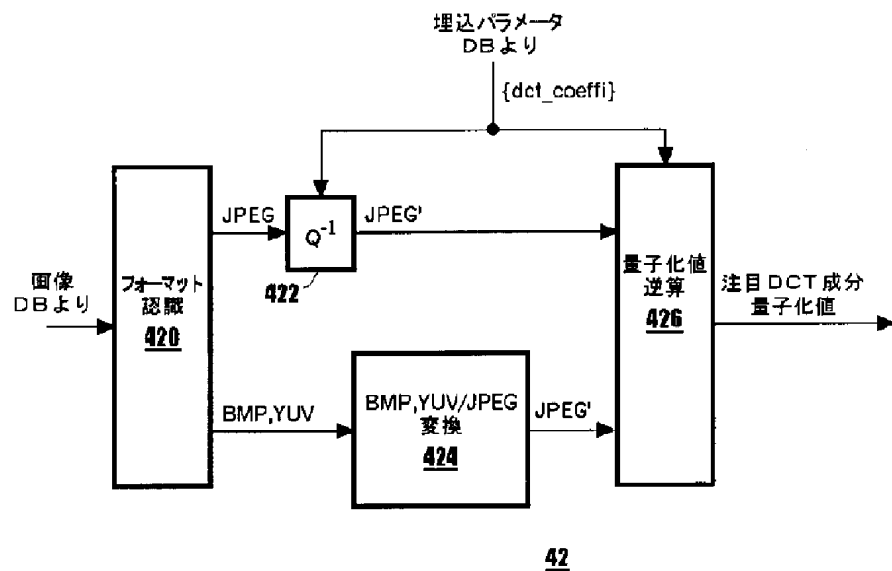


【図2】



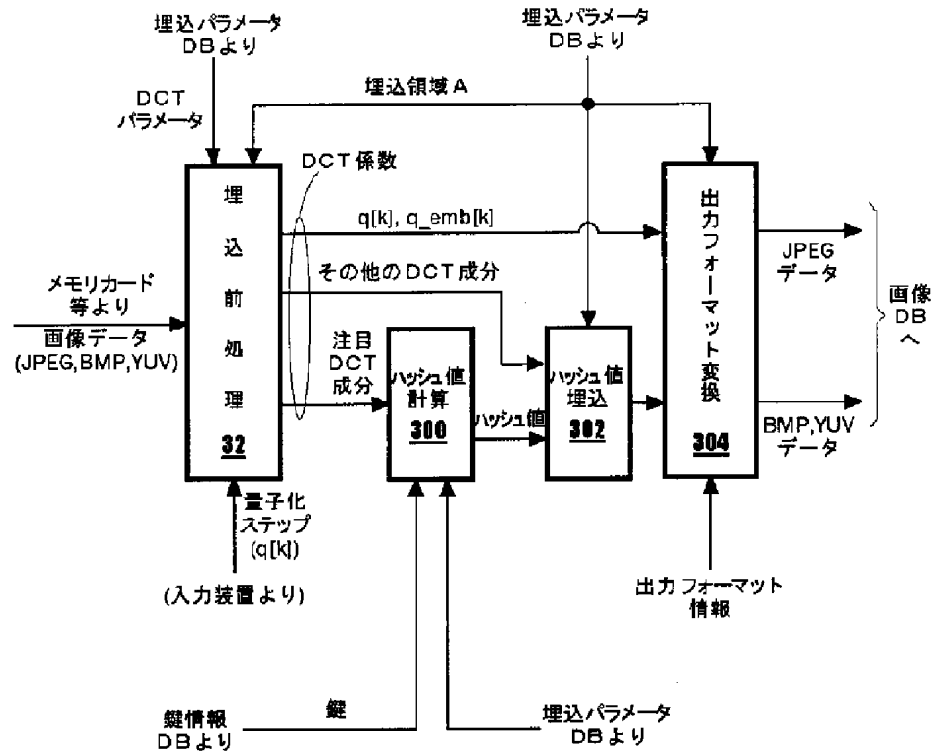
2

【図8】



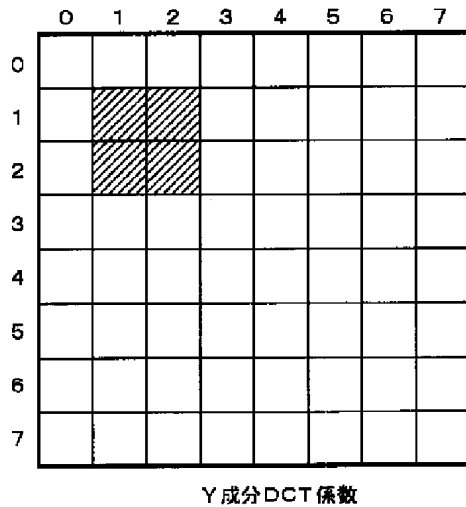
42

【図3】



30

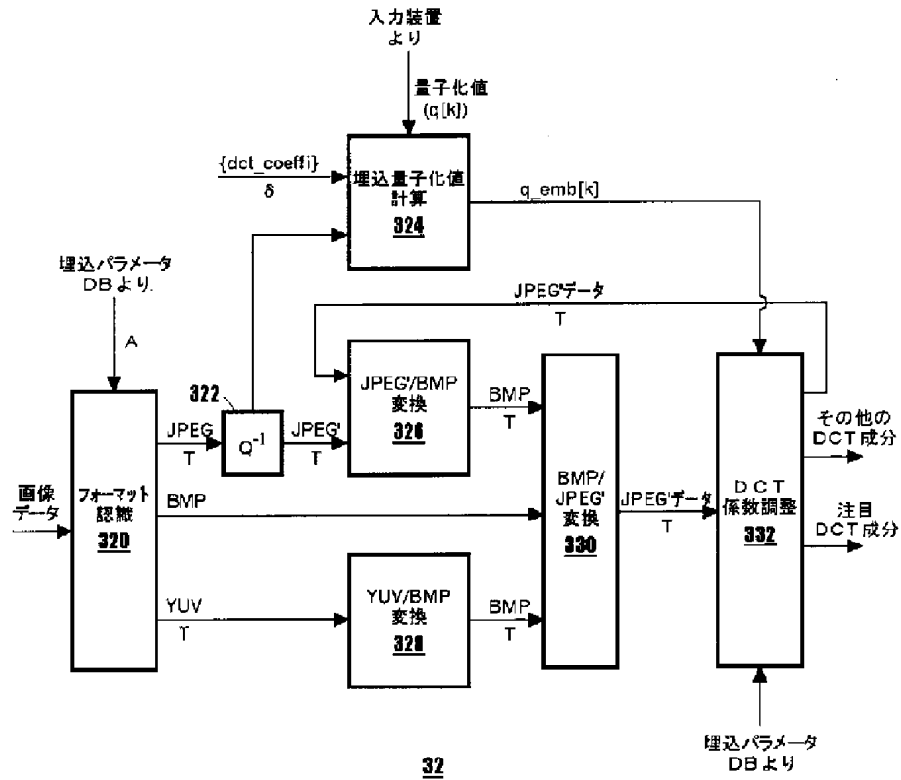
【図4】



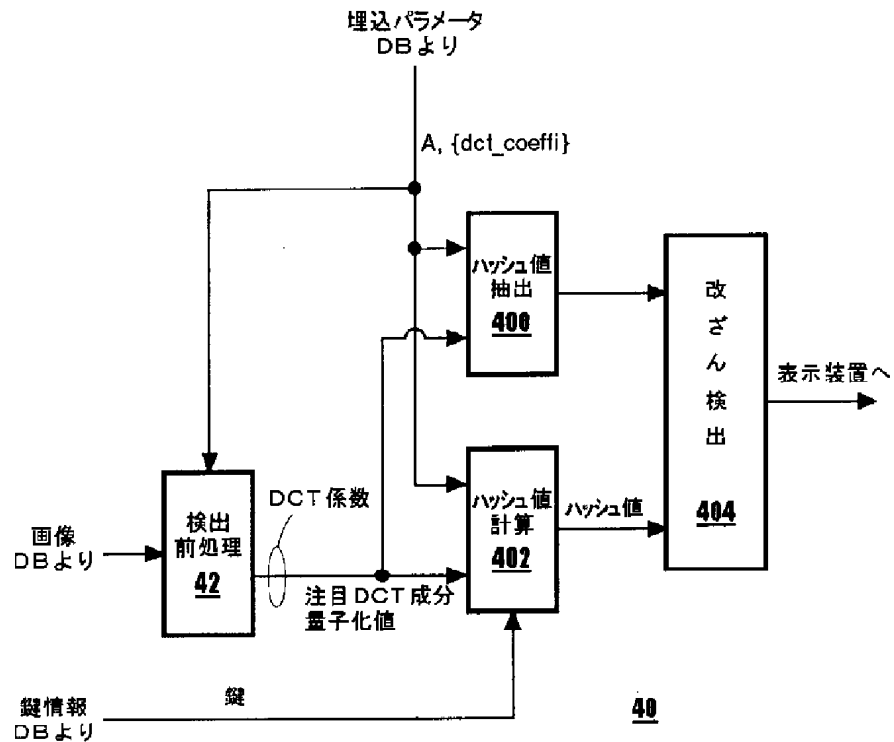
■ 注目するDCT成分



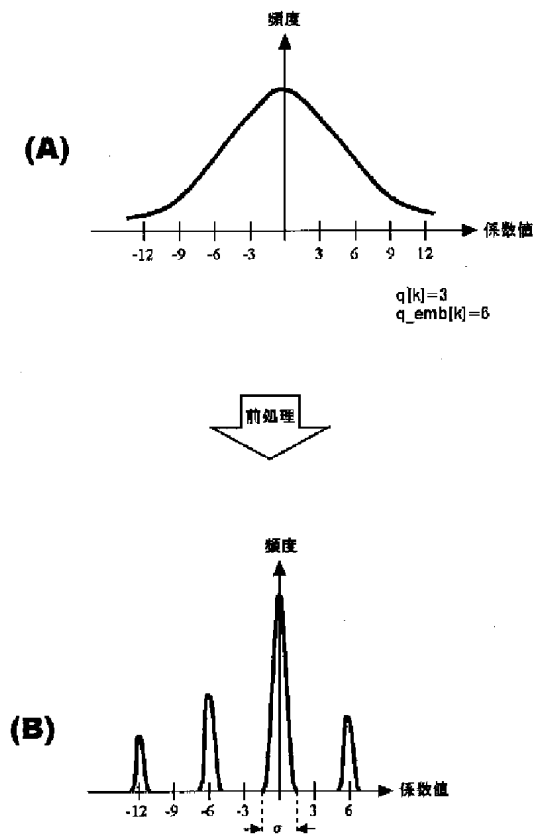
【図5】



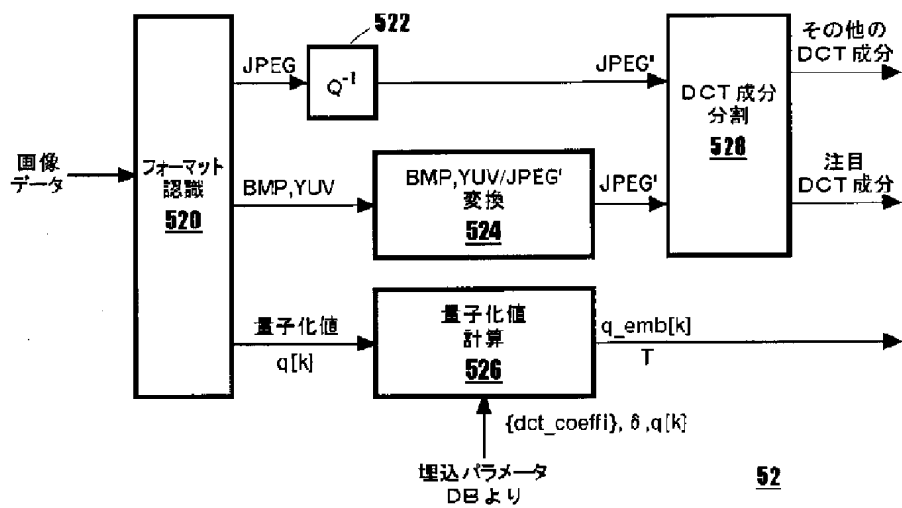
【図7】



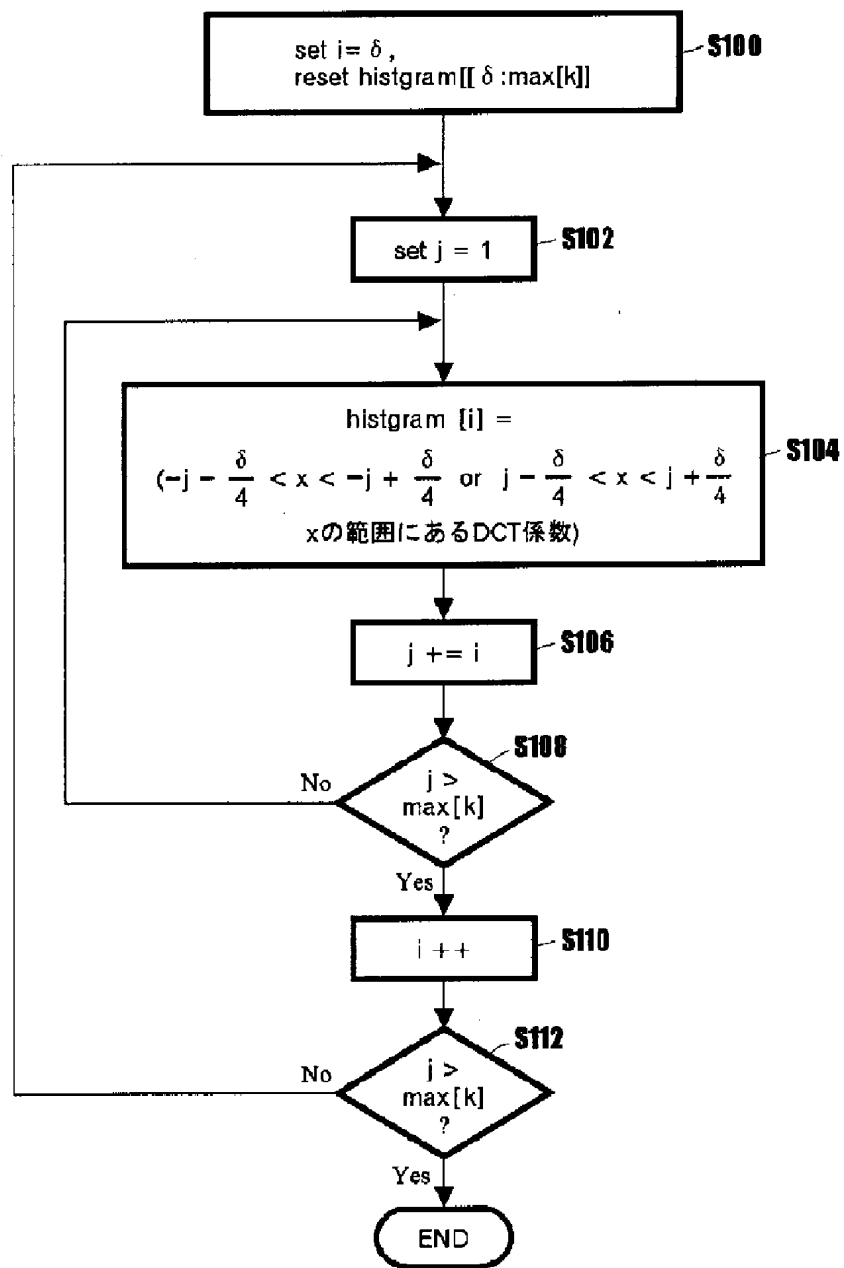
【図6】



【図14】

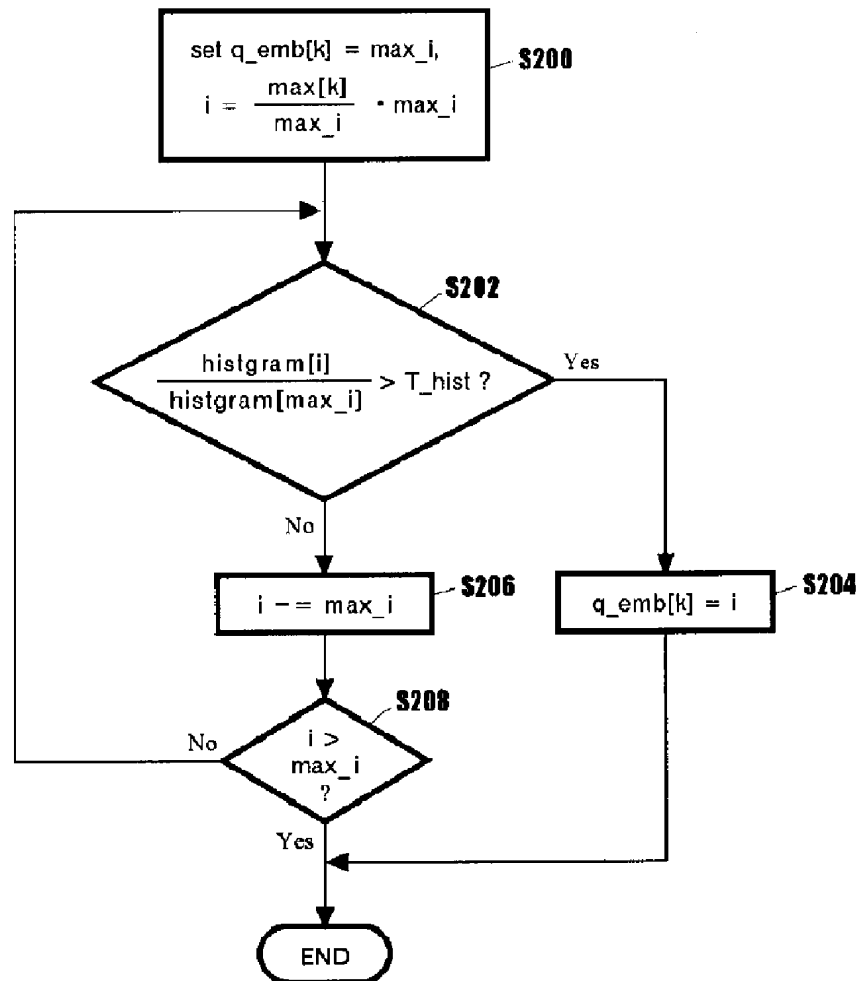


【図9】



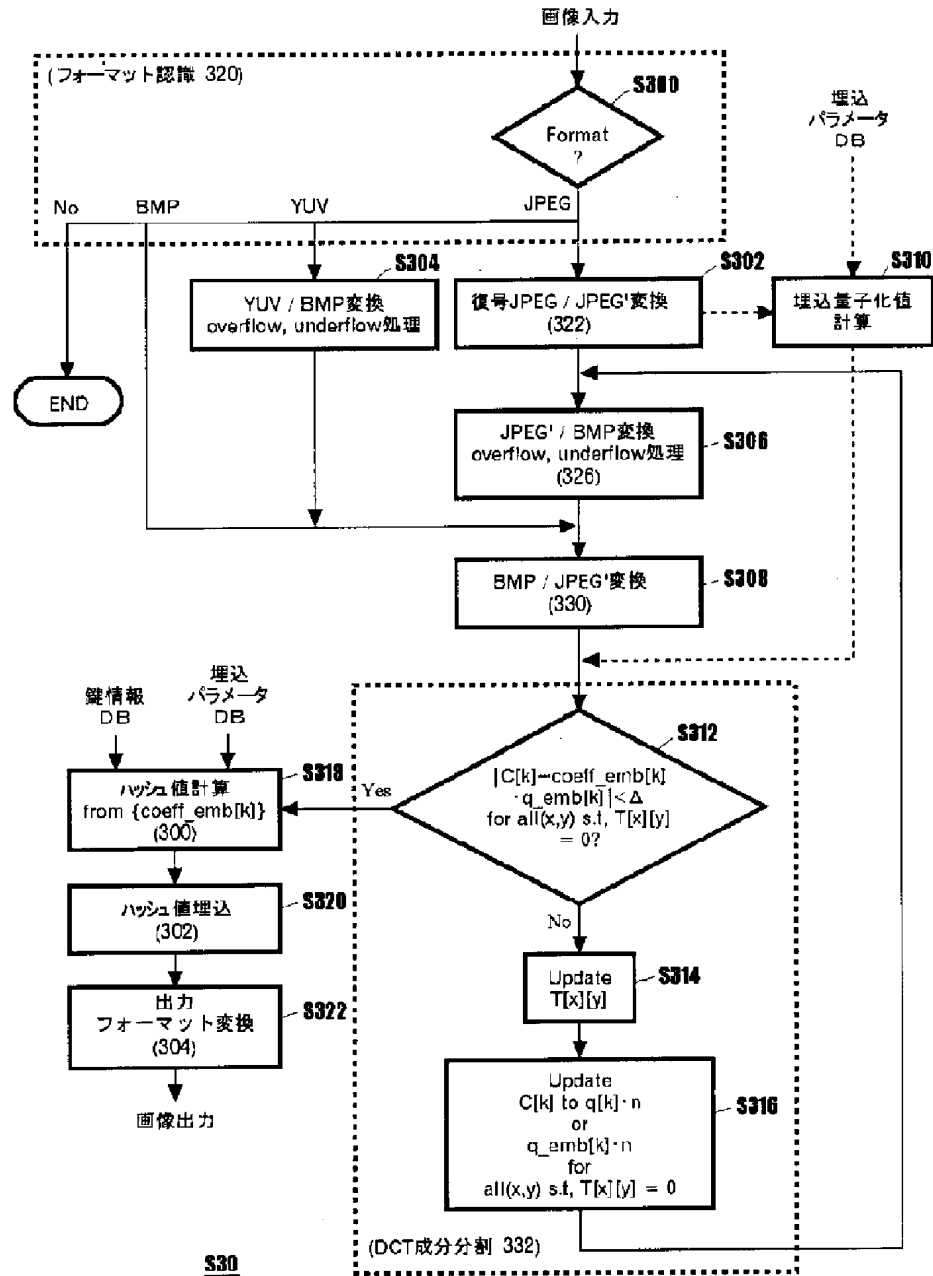
**S10**

【図10】

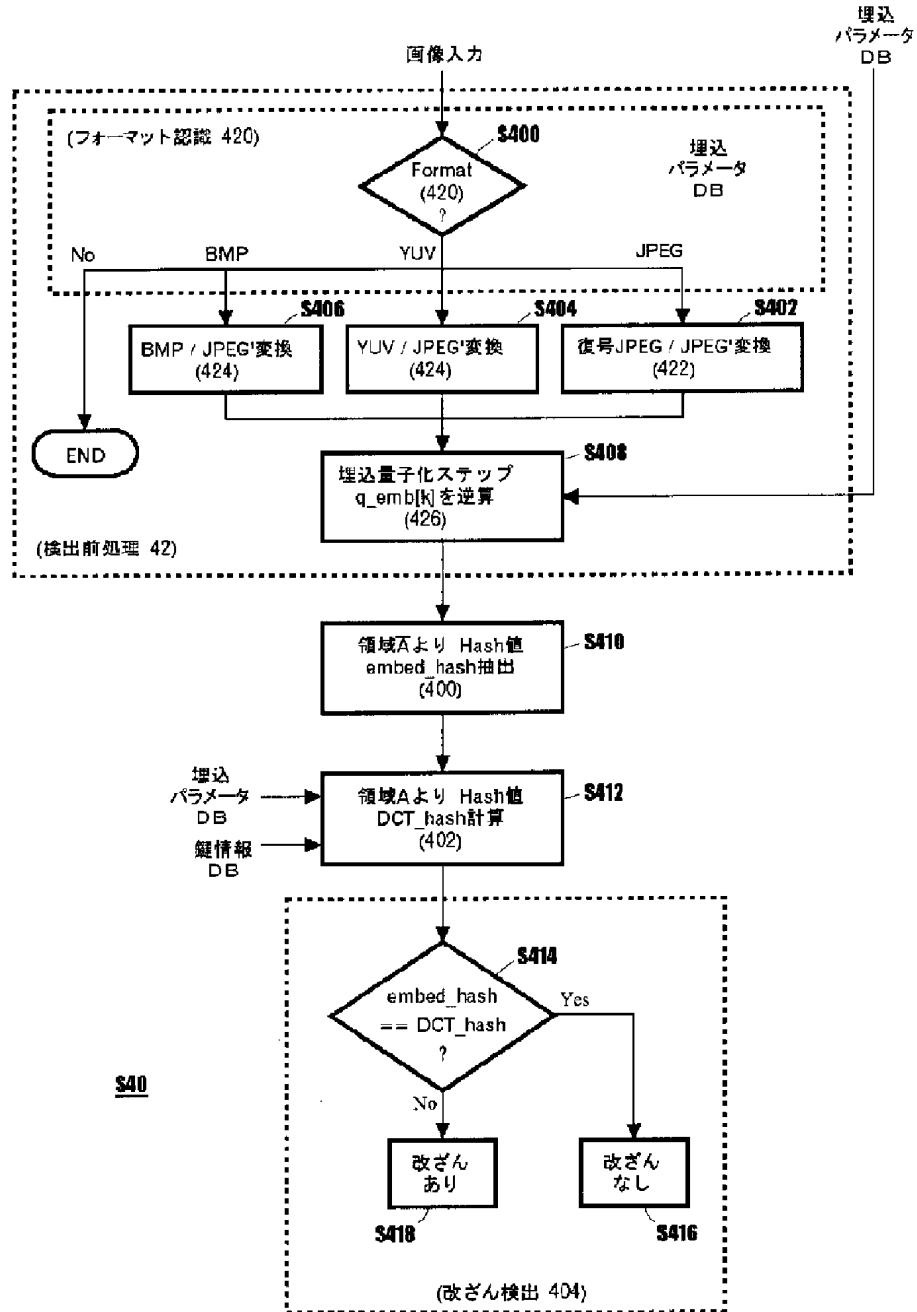


**S20**

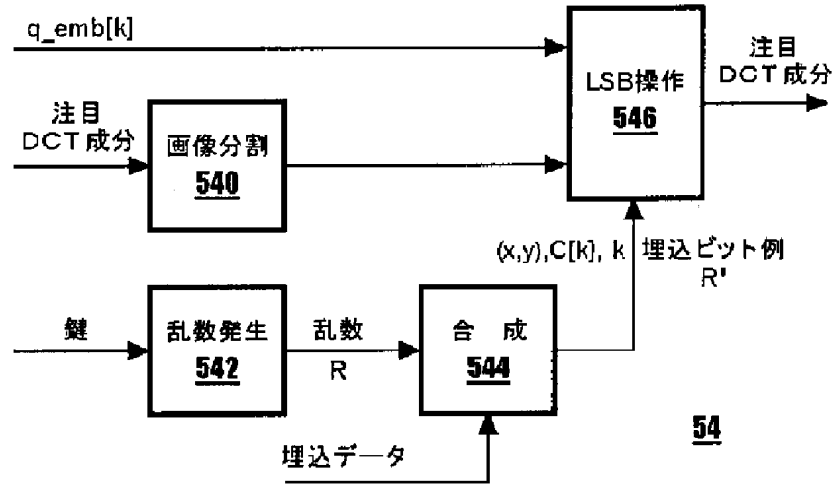
【図11】



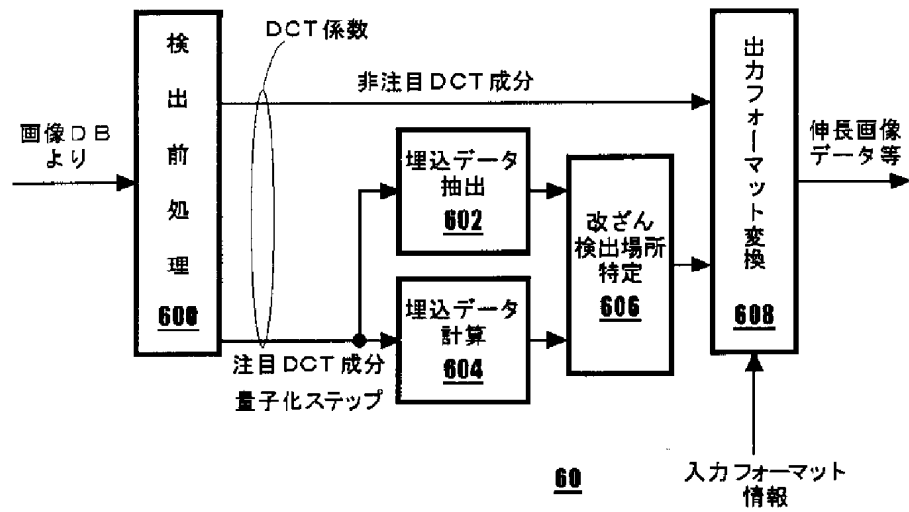
【図12】



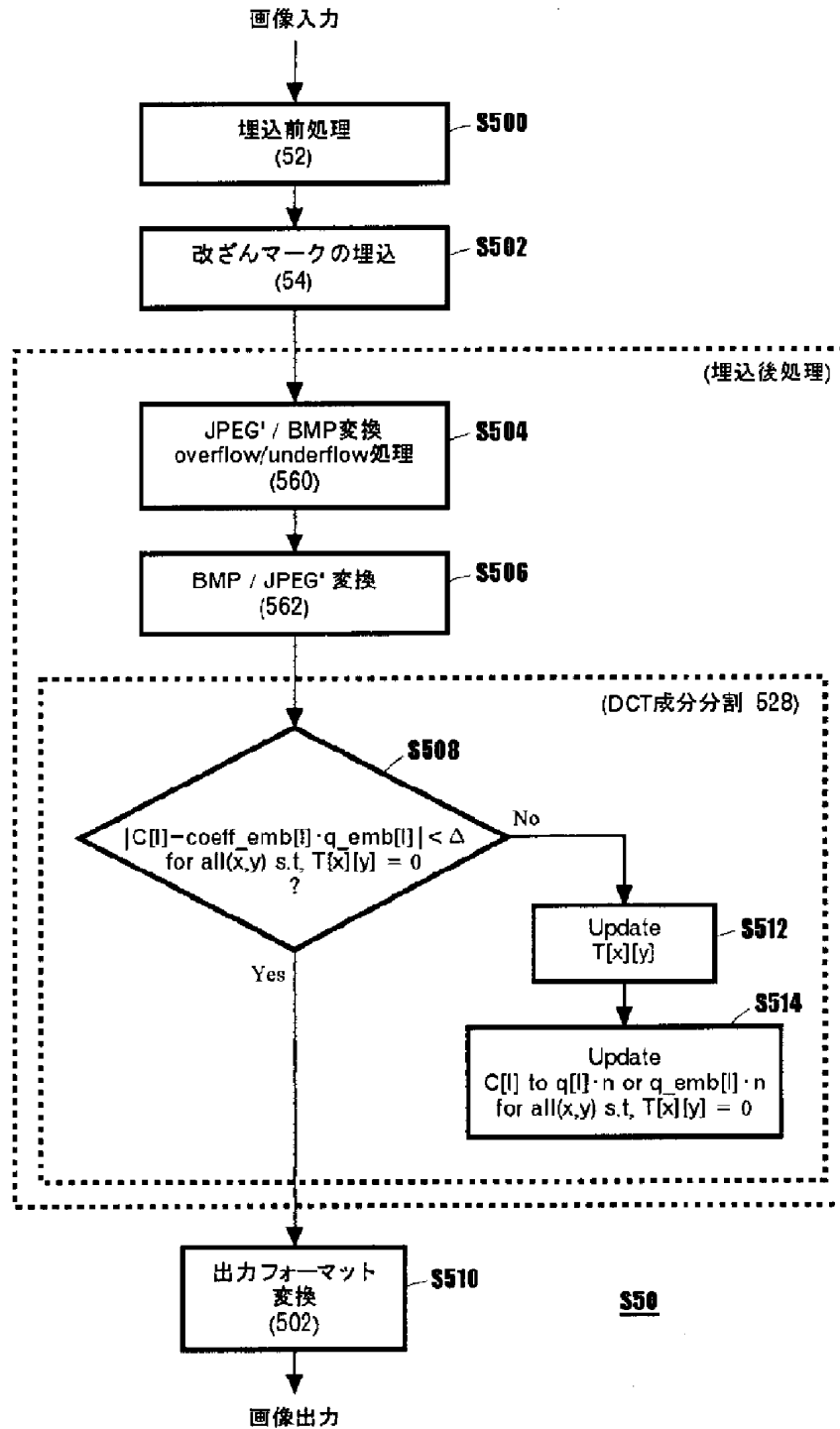
【図15】



【図17】

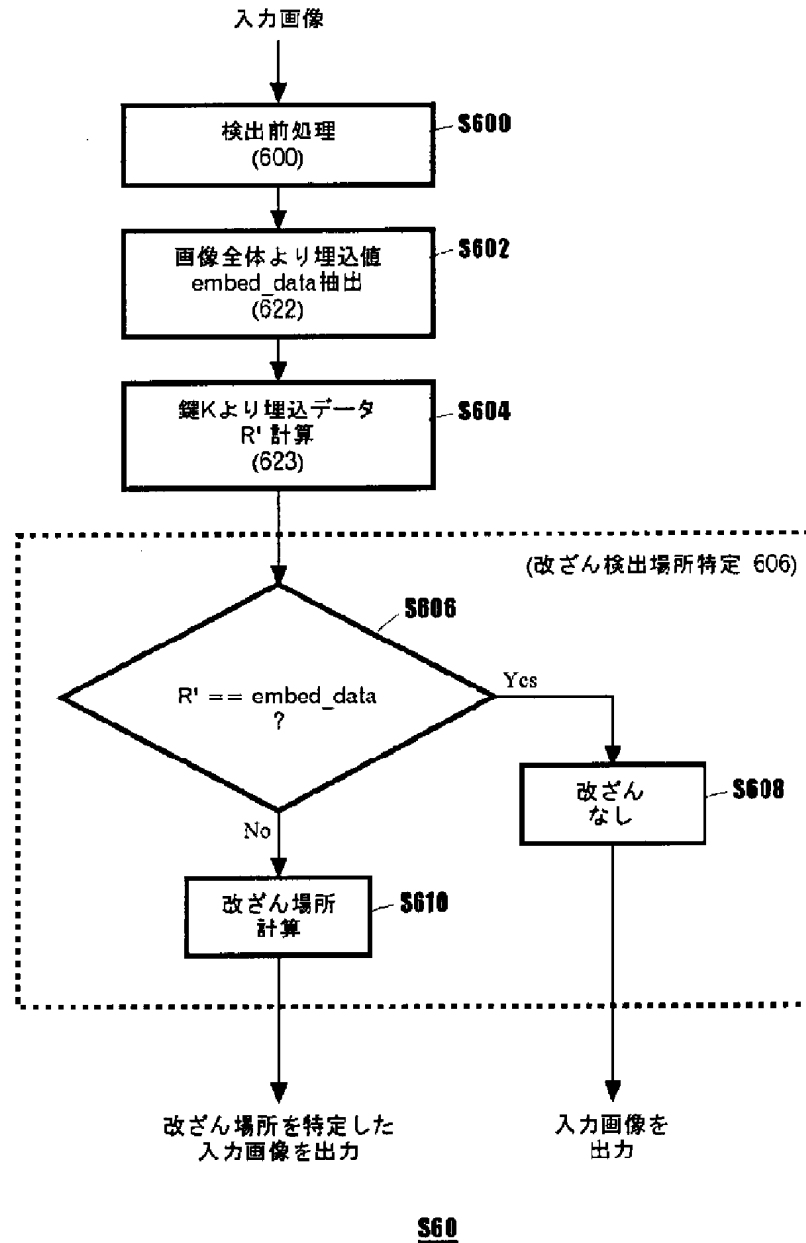


【図18】





【図19】



フロントページの続き

(51) Int. Cl. <sup>7</sup>  
H 0 4 N 7/30

識別記号

F I  
H 0 4 N 7/133

テーマコード (参考)  
Z 5 C 0 7 8

(72) 発明者 上條 浩一  
神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 東京基礎研究所  
内

(72) 発明者 森本 典繁  
神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 東京基礎研究所  
内

(72)発明者 利根川 聡子  
神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 東京基礎研究所  
内

F ターム(参考) 5B057 AA11 CA01 CA08 CA12 CA16  
CB01 CB08 CB12 CB16 CB19  
CE08 CG05 CG09 CH01 CH11  
5C053 FA08 FA13 FA27 GB06 GB07  
GB21 GB22 GB26 GB33 GB36  
GB40 JA21 JA30 KA05 LA06  
5C059 KK35 KK43 LA02 MA00 MA23  
MD02 PP01 PP14 RC35 SS15  
SS20  
5C076 AA14 AA36 AA40 BA06 BA09  
5C077 LL14 MP08 NP01 PP21 PP23  
PQ12 PQ22 RR21 RR30  
5C078 AA09 BA57 CA14 CA47 DA01  
DA02